Docket No. 247926US6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Atsushi HAMANO GAU:

SERIAL NO: New Application EXAMINER:

FILED: Herewith

FOR: DATA SENDING/RECEIVING SYSTEM FOR ENABLING DoS COUNTERMEASURE

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-016641	January 24, 2003

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Registration No. 40,073

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

5049011 6 ﾁｬｸ00
(5911)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月２４日

出願番号
Application Number: 特願２００３－０１６６４１

[ST. 10/C]: [ＪＰ２００３－０１６６４１]

出願人
Applicant(s): ソニー株式会社

２００３年１１月１９日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０９５６９１

【書類名】　特許願
【整理番号】　0290767904
【提出日】　平成15年 1月24日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内
　【氏名】　濱野　淳史
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082740
　【弁理士】
　【氏名又は名称】　田辺　恵基
【手数料の表示】
　【予納台帳番号】　048253
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9709125
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　送信装置及び受信装置

【特許請求の範囲】

【請求項１】

所定の通信プロトコルに準拠して生成された送信パケットを順次ネットワークを介して送信する送信手段と、

上記送信パケットの送信対象である受信側から要求があった期間のみ、当該受信側だけに識別させるための識別情報を各上記送信パケットに付加する識別情報付加手段と

を具えることを特徴とする送信装置。

【請求項２】

上記識別情報生成手段は、

上記送信パケットの送り出し方向に未符号化状態で上記識別情報を付加する

ことを特徴とする請求項１に記載の送信装置。

【請求項３】

上記識別情報は、

所定の擬似乱数と、当該擬似乱数に固有のシーケンス番号情報とでなる

ことを特徴とする請求項１に記載の送信装置。

【請求項４】

所定の通信プロトコルに準拠して生成された送信パケットを順次ネットワークを介して送信する第１のステップと、

上記送信パケットの受信側から要求があった期間のみ、当該受信側だけに識別させるための識別情報を各上記送信パケットに付加する第２のステップと

を具えることを特徴とする送信方法。

【請求項５】

送信側からネットワークを介して順次送信され、所定の通信プロトコルに準拠した送信パケットを受信する受信手段と、

上記受信手段が受信した各上記送信パケットのうち、当該パケットの内容が変更された上記送信パケットである内容変更パケットを検出する検出手段と、

上記検出手段により検出された上記内容変更パケットの受信状況に応じて、上記検出手段だけに識別させるための識別情報の上記送信パケットへの付加を上記送信側に要求する要求手段と

を具えることを特徴とする受信装置。

【請求項６】

上記要求手段は、

上記内容変更パケットに係る上記送信パケットを送信する上記送信側に対してのみ上記識別情報の付加を要求する

ことを特徴とする請求項６に記載の受信装置。

【請求項７】

送信側からネットワークを介して順次送信され、所定の通信プロトコルに準拠した送信パケットを受信する第１のステップと、

上記第１のステップで受信された各上記送信パケットのうち、当該パケットの内容が変更された上記送信パケットである内容変更パケットを検出する第２のステップと、

上記第２のステップで検出された上記内容変更パケットの受信状況に応じて、上記検出手段だけに識別させるための識別情報の上記送信パケットへの付加を上記送信側に要求する第３のステップと

を具えることを特徴とする受信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は送信装置及び受信装置に関し、例えばインターネットを介して送信装置と受信装置とが接続されてなる送受信システムに適用して好適なものである。

【０００２】

【従来の技術】

従来、本出願人によって既に開示した特願2002-263272号に係る送受信システムは、送信側では送信対象の暗号パケットを送信する際に、受信装置だけに正当性を証明するための正当性証明情報を未暗号化状態で付加した後にインターネッ

トを介して送信し、一方受信側では当該暗号パケットに付加された正当性証明情報の正当性が維持されている判定結果が得られた場合にのみ暗号パケットを復号する。

【０００３】

従って送受信システムは、サービス妨害（DoS:Denial of Service)行為のうち、暗号パケットの送信元アドレス等を書き換えることにより生成された詐称パケットを大量に受信装置へ送信する行為があった場合、当該受信装置では第三者の知り得ない正当性証明情報に基づいて詐称パケットを復号する前に破棄することができ、かくして、大量の詐称パケットを受信した場合であっても迅速な処理を実現することができるようになされている。

【０００４】

【発明が解決しようとする課題】

ところがかかる構成の送受信システムにおいては、サービス妨害行為の有無に係わらず常に正当性証明情報を暗号パケットに付加して送信することにより、当該サービス妨害行為がなかった場合におけるシステム全体の処理負荷が顕著に増大し、その結果、システム全体としての送信効率が悪化してしまうという問題があった。

【０００５】

本発明は以上の点に考慮してなされたもので、システム全体としての送信効率を向上し得る送信装置、送信方法、受信装置及び受信方法を提案しようとするものである。

【０００６】

【課題を解決するための手段】

かかる課題を解決するため本発明においては、所定の通信プロトコルに準拠して生成された送信パケットを順次ネットワークを介して送信し、当該送信パケットの送信対象である受信側から要求があった期間のみ、当該受信側だけに識別させるための識別情報を各送信パケットに付加する。

【０００７】

この場合、受信側から要求があった期間以外については識別情報を各送信パケ

ットに付加しない分だけ送信手段、正当性付加手段及びネットワーク上に介在する中間ノードに対する処理負荷を低減することができる。

【０００８】

また、かかる課題を解決するため本発明においては、送信側からネットワークを介して順次送信され、所定の通信プロトコルに準拠した送信パケットを受信し、当該受信された各送信パケットのうち、当該パケットの内容が変更された送信パケットである内容変更パケットを検出し、当該検出した内容変更パケットの受信状況に応じて、検出手段だけに識別させるための識別情報の送信パケットへの付加を送信側に要求する。

【０００９】

この場合、送信側に要求しない際に送信側からは識別情報の付加された送信パケットが送信されない分だけ送信装置及びネットワーク上に介在する中間ノードに対する処理負荷を低減することができる。

【００１０】

【発明の実施の形態】

以下図面について、本発明の一実施の形態を詳述する。

【００１１】

（１）全体構成

図１において、１は全体として本発明を適用した送受信システムを示し、送信装置２、受信装置３及び通信妨害装置４がインターネット５に接続されており、当該送信装置２と受信装置３とがインターネット５を介して各種データの授受を行い得るようになされている。

【００１２】

送信装置２は、送信対象データを所定長のデータ片に分割し、当該データ片に対して所定の通信プロトコルに従ってパケット暗号化処理を施し、その結果順次生成される送信パケットＰＫ（ＰＫ１、ＰＫ２、……）を受信装置３へ送信する。

【００１３】

受信装置３は、送信装置２から送信される送信パケットＰＫを受信し、その送

信パケットＰＫに対して当該送信装置２と同一の通信プロトコルに従ってパケット復号処理を施し、その結果復元されるデータ片を例えば内部メモリ（図示せず）に記憶する。

【００１４】

通信妨害装置４は、受信装置３に対してサービス妨害（DoS:Denial of Service）行為を行うようになされており、具体的には送信装置２から受信装置３へ送信される送信パケットＰＫ（ＰＫ１、ＰＫ２、……）を監視し、当該送信中の送信パケットＰＫ（ＰＫ１、ＰＫ２、……、又はＰＫｎ）を不当に入手し、当該入手した送信パケットＰＫの内容を変更した送信パケット（以下、これを内容変更パケットと呼ぶ）ＦＰＫを生成し、これを大量に複製した後に順次受信装置３へ送信する。

【００１５】

ここで、受信装置３は、通信妨害装置４から送信される内容変更パケットＦＰＫを大量に受信すると、サービス妨害行為に対する対策（以下、これをサービス妨害対策と呼ぶ）の開始を要求する要求データＤＮａを生成し、これを送信装置２へ送信する。

【００１６】

この場合、送信装置２は、受信装置３から送信される要求データＤＮａを受信した以降に順次生成した送信パケットＰＫについては、受信装置３だけに正当性を証明する識別情報をサービス妨害対策として付加し、その結果順次得られる送信パケット（以下、これを、妨害対策パケットと呼ぶ）ＢＭＰＫ（ＢＭＰＫ１、ＢＭＰＫ２……）を順次受信装置３へ送信する。

【００１７】

受信装置３は、送信装置２から送信される妨害対策パケットＢＭＰＫ及び通信妨害装置４から送信される内容変更パケットＦＰＫのうち、当該妨害対策パケットＢＭＰＫだけを復元し、その結果得られるデータ片を内部メモリ（図示せず）に記憶し得るようになされている。

【００１８】

また受信装置３は、通信妨害装置４から送信される内容変更パケットＦＰＫが

少なくなると、サービス妨害対策の停止を要求する要求データＤＮｂを生成し、これを送信装置２へ送信する。

【００１９】

この場合、送信装置２は、受信装置３から送信される要求データＤＮｂを受信すると、当該要求データＤＮｂを受信した以降に順次生成した送信パケットＰＫについては識別情報を付加することなくそのまま受信装置３へ送信するようになされている。

【００２０】

このように送受信システム１は、受信装置３における内容変更パケットＦＰＫの受信状況に応じて、要求データＤＮ（ＤＮａ、ＤＮｂ）を介して識別情報ＪＰの付加の有無を要求することにより、当該内容変更パケットＦＰＫの受信数が多い（すなわちサービス妨害行為の規模が大きい）場合にのみ、送信パケットＰＫに識別情報を付加した妨害対策パケットＢＭＰＫをインターネット５を介して送信装置２と受信装置３との間で送受信し得るようになされている。

【００２１】

なお、図１の実施の形態における送受信システム１においては、インターネット５を介して当該送信装置２と同一構成の１又は２以上の送信装置が受信装置３に接続されている場合、受信装置３は、当該複数の送信装置（送信装置２も含む。以下同じ）のうち、内容変更パケットＦＰＫの生成元となった送信パケットＰＫを送信する送信装置２に対してのみ、要求データＤＮ（ＤＮａ、ＤＮｂ）を介して識別情報ＪＰの付加の有無を要求し得るようになされている。

【００２２】

（２）送信装置の構成

図２に示すように、パケット生成部１１は、内部メモリから読み出した又は外部から供給された送信対象データＤ１０を所定長でなる複数のデータ片に分割し、当該データ片に対して例えばＩＰsec (Internet Protocol security)と呼ばれる通信プロトコルに従ってパケット暗号化処理を施すようになされている。

【００２３】

具体的にパケット生成部１１は、ＩＰsec で規定される複数の暗号鍵情報、暗

号化アルゴリズムや認証アルゴリズム等の各種セキュリティ情報群（ＳＡ(Security Association)）のうち、受信装置３へ最初にアクセスした際に送信装置２と受信装置３とのアドレスに基づいて予め決定しておいた使用するＳＡ（以下、これを使用セキュリティと呼ぶ）に従ってデータ片を暗号化した後にヘッダを付加し、その結果順次生成される送信パケットＰＫ（ＰＫ１、ＰＫ２、……）を送信処理部１２に与える。

【００２４】

因みに、かかる送信パケットＰＫには、使用セキュリティを示すＳＰＩ(Security Parameter Index)と呼ばれるインデックス情報も含まれている。

【００２５】

送信処理部１２の識別情報付加部１３は、識別情報を付加しない第１のモード（以下、これを妨害対策停止モードと呼ぶ）である場合には、当該識別情報付加部１３自身における処理を停止した休止状態となる。

【００２６】

従ってパケット生成部１１から順次与えられる送信パケットＰＫ（ＰＫ１、ＰＫ２、……）はそのままインターフェイス（以下、これを送信側インターフェイスと呼ぶ）１５を介して受信装置３（図１）へ送信される。

【００２７】

これに対して識別情報付加部１３は、識別情報を付加する第２のモード（以下、これを妨害対策モードと呼ぶ）である場合、まず、図３に示すように、パケット生成部１１から与えられる送信パケットＰＫ（ＰＫ１、ＰＫ２、……）ごとに固有の識別情報ＪＰ（ＪＰ１、ＪＰ２、……）を生成する。

【００２８】

次いで識別情報付加部１３は、送信パケットＰＫの送り出し方向に未符号化状態で識別情報ＪＰを付加し、その結果順次生成される妨害対策パケットＢＭＰＫ（ＢＭＰＫ１、ＢＭＰＫ２……）を送信側インターフェイス１５を介して受信装置３（図１）へ送信する。

【００２９】

ここで、識別情報付加部１３は、識別情報ＪＰの具体的な生成手法として、予

め内部メモリ（図示せず）に格納されたＩＰsec の規定とは別に送信装置２と受信装置３とだけが独自に有する識別情報生成アルゴリズムにより、まずパケット生成部１１で用いられた暗号化鍵情報に基づいて種情報（シード）を導出する。

【００３０】

次いで識別情報付加部１３は、図４に示すように、種情報（シード）から通信妨害装置４には知り得ない固有の擬似乱数Ｇ（Ｇ１、Ｇ２、……）を生成し、当該擬似乱数Ｇの生成順番に対応するシーケンシャルな番号のデータ（以下、これをシーケンス番号と呼ぶ）Ｓ（Ｓ１、Ｓ２、……）を当該擬似乱数Ｇの例えば先頭に付加することにより識別情報ＪＰ（ＪＰ１、ＪＰ２、……）を生成する。

【００３１】

従って識別情報付加部１３は、擬似乱数Ｇとシーケンス番号Ｓとの対応関係を通信妨害装置４に対しては単に規則性のないデータ列として認識させ得るのみならず、当該擬似乱数Ｇとシーケンス番号Ｓとの組み合わせが２度と同一の状態となることはない識別情報ＪＰ（ＪＰ１、ＪＰ２、……）を生成することができ、かくして、を受信装置３に対してのみほぼ確実に識別させ得る信頼性の高い識別情報ＪＰとして生成し得るようになされている。

【００３２】

また識別情報付加部１３は、送信装置２と受信装置３とだけが独自に有する識別情報生成アルゴリズムに従って識別情報ＪＰを生成した後に未符号化状態で送信パケットＰＫに付加しているので、当該送信パケットＰＫの復号前に当該識別情報ＪＰを受信装置３（図１）に対してのみ認識させ得るようになされている。

【００３３】

送信処理部１２のフィードバック受信部１４は、受信装置３（図１）から送信される要求データＤＮ（ＤＮａ，ＤＮｂ）を受信するようになされており、サービス妨害対策を開始させる要求データＤＮａを受信した場合には、識別情報付加部１３を妨害対策モードに遷移させる。

【００３４】

これに対してフィードバック受信部１４は、サービス妨害対策を停止させる要求データＤＮｂを受信した場合には、識別情報付加部１３を妨害対策停止モード

に遷移させる。

【００３５】

このように送信処理部１２は、要求データＤＮａを受信してから要求データＤＮｂを受信するまでの期間のみ識別情報付加部１３を動作させることにより、当該識別情報付加部１３におけるデータ処理負荷を低減し得るようになされている。

【００３６】

ところで送信処理部１２の送信処理においては、送信装置２内のプログラム格納用メモリ（図示せず）に予め格納された所定の送信プログラムを送信装置２内におけるワークメモリ（図示せず）上に読み出して展開した送信装置２内のＣＰＵ（図示せず）と、当該送信処理部１２とが協動して実現するようになされており、当該送信処理手順の説明については後述する。

【００３７】

（３）受信装置の構成

図５に示すように、パケット受信部２２は、インターネット５（図１）及びインターフェイス（以下、これを受信側インターフェイスと呼ぶ）２１を順次介してパケット（送信パケットＰＫ、妨害対策パケットＢＭＰＫ又は内容変更パケットＦＰＫ）を受信し、これを受信処理部２３に与える。

【００３８】

受信処理部２３の攻撃検出部２４は、複数の送信装置からパケットを送信し始めるための所定のアクセスがあった際に予め当該送信装置との間で個々に使用セキュリティを決定し、各送信装置にそれぞれ対応する使用セキュリティを把握しておくようになされている。

【００３９】

従って攻撃検出部２４は、パケット受信部２２から与えられるパケットについて、当該パケットの送信元アドレスと、当該パケットに含まれるインデックス情報（ＳＰＩ）とに基づいて当該パケットに用いられた使用セキュリティを検索し、当該検索した使用セキュリティに対応する例えば送信装置２を特定し得るようになされている。

【００４０】

この状態において攻撃検出部２４は、特定した送信装置２に対してサービス妨害対策の開始要求をしていない場合には、当該送信装置２から識別情報ＪＰが付加されない状態で送信される送信パケットＰＫに対して、第１のモード（以下、これを第１の攻撃検出モードと呼ぶ）でパケット復号処理を実行する。

【００４１】

具体的に攻撃検出部２４は、送信装置２から送信される送信パケットＰＫを、当該送信装置２に対応する使用セキュリティに従って復号する。

【００４２】

ここで例えば本来得られるべきハッシュ値が得られない等の復号エラーが生じた場合には、攻撃検出部２４は、送信装置２から送信された送信パケットＰＫの内容が変更された内容変更パケットＦＰＫであることを検出し、当該内容変更パケットＦＰＫの本来の送信元が送信装置２であることをフィードバック制御部２５に通知すると共に、当該内容変更パケットＦＰＫを破棄する。

【００４３】

これに対して攻撃検出部２４は、送信パケットＰＫを復号した結果、送信パケットＰＫに含まれる暗号化データ片（図３）を復元した場合には、当該データ片を送信装置２のデータ片として内部メモリに記憶する。

【００４４】

一方、攻撃検出部２４は、送信装置２にサービス妨害対策の開始要求をしている場合には、当該送信装置２から識別情報ＪＰが付加された状態で送信される妨害対策パケットＢＭＰＫ（図３）に対して、第２のモード（以下、これを第２の攻撃対策モードと呼ぶ）でパケット復号処理を実行する。

【００４５】

具体的に攻撃検出部２４は、当該送信装置２から送信される妨害対策パケットＢＭＰＫ（図３）の先頭に識別情報ＪＰが付加されているか否かを判定する。

【００４６】

そして攻撃検出部２４は、識別情報ＪＰが付加されている肯定結果が得られた場合には第２段階として、識別情報ＪＰのシーケンス番号Ｓ（図４）について、

予め内部メモリ（図示せず）に複数の送信装置単位で一旦記憶しておいた過去の識別情報ＪＰのシーケンス番号Ｓとは異なるか否かを判定する。

【００４７】

さらに攻撃検出部２４は、過去に受け取った識別情報ＪＰのシーケンス番号Ｓと異なっている肯定結果が得られた場合には第３段階として、送信装置２と同一の識別情報生成アルゴリズムにより、送信装置２と同一の種情報（シード）を用いて識別情報ＪＰと比較するための比較用識別情報を生成した後、当該識別情報ＪＰと比較用識別情報とを照合した結果が一致するか否かを判定する。

【００４８】

ここで、第１段階で否定結果が得られた場合には、サービス妨害の開始を送信装置２に要求したにもかかわらず識別情報ＪＰが付加されていないので、送信パケットＰＫの内容を変更した不当な内容変更パケットＦＰＫであることを表わす。

【００４９】

また第２段階又は第３段階で否定結果が得られた場合には、妨害対策パケットＢＭＰＫにおける内容に変更のある不当な内容変更パケットＦＰＫであることを表わす。

【００５０】

従って攻撃検出部２４は、第１段階、第２段階又は第３段階のいずれか１つでも否定結果が得られた場合には内容変更パケットＦＰＫであることを検出し、当該内容変更パケットＦＰＫの本来の送信元が送信装置２であることをフィードバック制御部２５に通知すると共に、当該内容変更パケットＦＰＫを破棄する。

【００５１】

これに対して攻撃検出部２４は、第１段階、第２段階又は第３段階のいずれについても肯定結果が得られた場合には、当該送信装置２に対応する使用セキュリティに従って送信パケットＰＫを復号し、その結果復元されるデータ片を送信装置２のデータとして内部メモリに記憶する。

【００５２】

このように攻撃検出部２４は、第１の攻撃検出モードにおいて、パケット受信

部２２から順次与えられるパケット毎に使用セキュリティを検索し、当該使用セキュリティに対応する送信装置を特定した後に復号することにより、正規の送信パケットに係るデータ片を複数の送信装置毎に内部メモリ上で管理すると共に、当該複数の送信装置毎に内容変更パケットＦＰＫを検出し得るようになされている。

【００５３】

また攻撃検出部２４は、第２の攻撃検出モードにおいて、第１の攻撃検出モードと同様にして送信装置を特定した後に、送信パケットＰＫの先頭に未符号化状態で付加された識別情報ＪＰに基づいて内容変更パケットＦＰＫであるか否かを判定することにより、当該送信パケットＰＫの復号前に複数の送信装置毎に内容変更パケットＦＰＫを検出し得るようになされている。

【００５４】

従って攻撃検出部２４は、通信妨害装置４から大量の内容変更パケットＦＰＫを受信した場合であっても、当該大量の内容変更パケットＦＰＫをそれぞれ復号するまでもなく処理負荷の小さい簡易な処理によって破棄することができ、これにより受信装置３における処理負荷を格段に低減することができるようになされている。

【００５５】

受信処理部２３のフィードバック制御部２５は、複数の送信装置ごとにカウンタを有し、攻撃検出部２４から内容変更パケットＦＰＫの本来の送信元である送信装置が通知される度に当該通知に対応する送信装置のカウンタを順次「１」ずつ繰り上げると共に、当該各カウンタにおける所定の単位時間当たりの繰り上げ数（以下、これを単位攻撃回数と呼ぶ）を内部クロックに基づいて計測する。

【００５６】

かかる単位攻撃回数は、その数値が大きい場合には内容変更パケットＦＰＫを大量に受信している、すなわちサービス妨害行為の規模が大きいことを表し、これに対して当該数値が小さい場合にはサービス妨害行為の規模が比較的小さいことを表す。

【００５７】

またフィードバック制御部２５は、カウンタの単位攻撃回数が所定の閾値よりも大きくなったとき、当該カウンタに対応する送信装置のサービス妨害対策の開始命令をフィードバック送信部２６に与えると共に、当該送信装置に係るパケットを攻撃検出部２４がパケット復号処理を実行する際に第２の攻撃対策モードで実行させる。

【００５８】

これに対してフィードバック制御部２５は、カウンタの単位攻撃回数が所定の閾値よりも小さくなったとき、当該カウンタに対応する例えば送信装置のサービス妨害対策の停止命令をフィードバック送信部２６に与えると共に、当該送信装置に係るパケットを攻撃検出部２４がパケット復号処理を実行する際に第１の攻撃対策モードで実行させる。

【００５９】

かかる所定の閾値は、受信装置３の処理能力に応じて変更され、復号モードを実行する受信装置３が内容変更パケットＦＰＫを大量に受けたことにより無駄に消費される処理負荷によって受信装置３が動作不能となってしまう単位攻撃回数のおよそ１０％～２０％が選定される。

【００６０】

このようにフィードバック制御部２５は、カウンタの単位攻撃回数に応じて攻撃検出部２４における処理状態を切り換え得るようになされている。

【００６１】

フィードバック送信部２６は、フィードバック制御部２５から与えられる命令に応じた要求データＤＮ（ＤＮａ又はＤＮｂ）を生成し、これを受信側インターフェイス２１を介して例えば送信装置２（図１）へ送信する。

【００６２】

かかる要求データＤＮ（ＤＮａ及びＤＮｂ）としては、ＲＦＣ(Request for Comments) と呼ばれる仕様書群のうち、例えば図６に示すように、ＲＦＣ７９２において規定されるＩＣＭＰ(Internet Control Message Protocol) を適用するようになされている。

【００６３】

この場合、「ｃｏｄｅ」には、「０」又は「１」が記述され、当該「１」であった場合にはサービス妨害対策の開始要求を表すと共に「０」であった場合にはサービス妨害対策の停止要求を表すようになされており、送信装置２では、当該「ｃｏｄｅ」に記述された「０」又は「１」に基づいてサービス対策の開始又は停止要求を認識し得るようになされている。

【００６４】

因みに「ｔｙｐｅ」には、受信装置３と受信装置２との間でそれぞれ認識し得る値が記述され、また「ｃｈｅｃｋｓｕｍ」には、通信データＤＮが壊れているか否かを送信装置２がチェックするためのデータ列が記述されるようになされている。

【００６５】

このように受信処理部２３は、複数の送信装置毎に内容変更パケットＦＰＫをカウントして単位攻撃回数を計測し、当該計測結果が所定の閾値を上回ったとき又は下回った送信装置に対してのみ要求データＤＮ（ＤＮａ及びＤＮｂ）を送信することにより、複数の送信装置のうち内容変更パケットＦＰＫの本来の送信元である送信装置に対してのみサービス妨害対策を開始又は停止させ得るようになされている。

【００６６】

ところで受信処理部２３の受信処理においては、送信プログラムに対応する受信プログラムが予め受信装置３内のプログラム格納用メモリ（図示せず）に格納されており、当該受信プログラムを受信装置３内におけるワークメモリ（図示せず）上に読み出して展開した受信装置３内のＣＰＵ（図示せず）と、受信処理部２３とが協動して実現するようになされている。

【００６７】

以下、送信処理部１２における送信処理手順と、受信処理部２３における受信処理手順とをそれぞれフローチャートを用いて説明する。

【００６８】

（４）送信処理手順及び受信処理手順

（４－１）送信処理手順

まずは、送信処理部１２における送信処理手順について図７に示すフローチャートを用いて説明する。

【００６９】

すなわち送信処理部１２は、例えば送信対象データＤ１を受信装置３へ送信する所定の送信操作が行われると、ルーチンＲＴ１の開始ステップＳＰ０から次のステップＳＰ１へ移る。

【００７０】

ステップＳＰ１において送信処理部１２は、識別情報付加部１３を妨害対策停止モードにし、次のステップＳＰ２へ移る。

【００７１】

この場合、識別情報付加部１３は休止状態にあり、従ってパケット生成部１１から与えられる送信パケットＰＫは、識別情報ＪＰ（図４）を付加するこなくそのまま送信側インターフェイス１５に与えられる。

【００７２】

ステップＳＰ２において送信処理部１２は、フィードバック受信部１４により、受信装置３（図１）から送信される要求データＤＮ（ＤＮａ，ＤＮｂ）を受信したか否かを判定する。ここで否定結果が得られると、このことは未だ要求データＤＮを受信していないことを表しており、このとき送信処理部１２は当該要求データＤＮを受信するまで待ち受ける。

【００７３】

これに対してステップＳＰ２で肯定結果が得られると、このことは要求データＤＮを受信したことを表しており、このとき送信処理部１２は、次のステップＳＰ３へ移る。

【００７４】

ステップＳＰ３において送信処理部１２は、フィードバック受信部１４により、ステップＳＰ２で受信した要求データＤＮのデータ内容に基づいて、受信装置３（図１）がサービス妨害行為を受けているか否かを判定する。

【００７５】

ここで肯定結果が得られると、このことは要求データＤＮの「ｃｏｄｅ」（図

６）に「１」が記述されている、すなわちサービス妨害対策の開始要求があったことを表しており、このとき送信処理部１２は、次のステップＳＰ４へ移る。

【００７６】

ステップＳＰ４において送信処理部１２は、フィードバック受信部１４により、識別情報付加部１３を妨害対策停止モードから妨害対策モードに遷移させた後、ステップＳＰ２へ戻って、要求データＤＮを受信するまで待ち受ける。

【００７７】

この場合、識別情報付加部１３は、パケット生成部１１から与えられる送信パケットＰＫに識別情報ＪＰ（図４）を付加して妨害対策パケットＢＭＰＫ（図３）を生成し、当該妨害対策パケットＢＭＰＫを送信側インターフェイス１５に与えるようになされている。

【００７８】

一方、ステップＳＰ３で否定結果が得られると、このことは要求データＤＮの「ｃｏｄｅ」（図６）に「０」が記述されている、すなわちサービス妨害対策の停止要求があったことを表しており、このとき送信処理部１２は、次のステップＳＰ５へ移る。

【００７９】

ステップＳＰ５において送信処理部１２は、フィードバック受信部１４により、識別情報付加部１３が妨害対策モードである場合には、当該識別情報付加部１３を妨害対策モードから妨害対策停止モードに遷移させた後、ステップＳＰ２へ戻って、要求データＤＮを受信するまで待ち受ける。

【００８０】

この場合、識別情報付加部１３は再び休止状態となり、従ってパケット生成部１１から与えられる送信パケットＰＫは、識別情報ＪＰ（図４）を付加するこなくそのまま送信側インターフェイス１５に与えられるようになされている。

【００８１】

（４－２）受信処理手順

次に、受信処理部２３における受信処理手順について図８に示すフローチャートを用いて説明する。

【００８２】

すなわち受信処理部２３は、ルーチンＲＴ２の開始ステップＳＰ１０から次のステップＳＰ１１へ移る。

【００８３】

ステップＳＰ１１において受信処理部２３は、攻撃検出部２４により、パケット（送信パケットＰＫ又は内容変更パケットＦＰＫ）を受け取ったか否かを判定する。

【００８４】

ここで否定結果が得られると、このことは未だパケット受信部２２がパケット受信していないことを表しており、このとき受信処理部２３は、当該パケットを受け取るまで待ち受ける。

【００８５】

これに対して肯定結果が得られると、このことはパケット受信部２２がパケットを受信したことを表しており、このとき受信処理部２３は、次のステップＳＰ１２へ移る。

【００８６】

ステップＳＰ１２において受信処理部２３は、ステップＳＰ１１で受け取ったパケットに基づいて、当該パケットの送信元である例えば送信装置２を特定し、次のステップＳＰ１３へ移る。

【００８７】

ステップＳＰ１３において受信処理部２３は、攻撃検出部２４により、ステップＳＰ１２で特定した送信装置２に対してサービス妨害対策を停止させている場合には第１の攻撃検出モードでパケット復号処理を実行し、これに対してサービス対策を開始させている場合には第２の攻撃検出モードでパケット復号処理を実行し、ステップＳＰ１１で受け取ったパケットが内容変更パケットＦＰＫであるか否かを判定する。

【００８８】

ここで否定結果が得られると、このことはステップＳＰ１１で受け取ったパケットについては、送信装置２（図１）から送信された正当な送信パケットＰＫ又

は妨害対策パケットＢＭＰＫであることを表しており、このとき受信処理部２３は、攻撃検出部２４により当該送信パケットＰＫ又は妨害対策パケットＢＭＰＫに含まれるデータ片を送信装置２のデータ片として内部メモリに記憶した後、ステップＳＰ１１に戻って再びパケットを受信するまで待ち受ける。

【００８９】

これに対してステップＳＰ１３で肯定結果が得られると、このことはステップＳＰ１１で受け取ったパケットが実際には通信妨害装置４（図１）から送信された不当な内容変更パケットＦＰＫであることを表しており、このとき受信処理部２３は、次のステップＳＰ１４へ移る。

【００９０】

ステップＳＰ１４において受信処理部２３は、攻撃検出部２４により、ステップＳＰ１３で判定した内容変更パケットＦＰＫを破棄すると共に、内容変更パケットＦＰＫの生成元が送信装置２であることをフィードバック制御部２５に通知した後、次のステップＳＰ１５へ移る。

【００９１】

ステップＳＰ１５において受信処理部２３は、フィードバック制御部２５により、攻撃検出部２４から通知された、すなわちステップＳＰ１２で特定した送信装置２に対応するカウンタを「１」つ分だけ繰り上げ、次のステップＳＰ１６へ移る。

【００９２】

ステップＳＰ１６において受信処理部２３は、ステップＳＰ１５で繰り上げたカウンタを計測する単位攻撃回数（単位時間当たりの繰り上げ数）が所定の閾値を越えているか否かを判定する。

【００９３】

ここで肯定結果が得られると、このことは送信装置２から送信されたパケット（送信パケットＰＫ又は妨害対策パケットＢＭＰＫ）の送信アドレス等が書き換えられて生成された内容変更パケットＦＰＫの受信量が多く、すなわちサービス妨害行為の規模が大きいことを表しており、このとき受信処理部２３は、次のステップＳＰ１７へ移る。

【００９４】

ステップＳＰ１７において受信処理部２３は、送信装置２にサービス妨害対策を停止させていた場合には、フィードバック送信部２６によりサービス妨害対策の開始を要求する要求データＤＮａを生成して受信側インターフェイス２１を介して送信装置２へ送信した後、ステップＳＰ１１に戻る。

【００９５】

これに対してステップＳＰ１６で否定結果が得られると、このことは送信装置２から送信されたパケット（送信パケットＰＫ又は妨害対策パケットＢＭＰＫ）の送信アドレス等が書き換えられて生成された内容変更パケットＦＰＫの受信量が少なくなった又は全くない、すなわちサービス妨害行為の規模が小さくなった又はサービス妨害行為が行われていないことを表しており、このとき受信処理部２３は、次のステップＳＰ１８へ移る。

【００９６】

ステップＳＰ１８において受信処理部２３は、送信装置２にサービス妨害対策を開始させていた場合には、フィードバック制御部２５により送信装置２に対応するカウンタをリセットすると共に、フィードバック送信部２６によりサービス妨害対策の停止を要求する要求データＤＮｂを生成して受信側インターフェイス２１を介して送信装置２へ送信した後、ステップＳＰ１１に戻る。

【００９７】

因みに受信処理部２３は、ステップＳＰ１７において送信装置２にサービス妨害対策を既に開始させていた場合、及びステップＳＰ１８において送信装置２にサービス妨害対策を既に停止させていた場合には何ら処理することなくステップＳＰ１１へ戻るようになされている。

【００９８】

（５）動作及び効果

以上の構成において、送信装置２は、送信手段としての送信側インターフェイス１５により、ＩＰsec に規定される暗号プロトコルに準拠して生成された送信パケットＰＫを順次インターネット５を介して送信する。

【００９９】

この状態において送信装置２は、識別情報付加手段としての識別情報付加部１３により、送信パケットＰＫの送信対象である受信装置３から要求があった期間（すなわち要求データＤＮａを受けてから当該要求データＤＮｂを受けるまでの期間）のみ識別情報ＪＰを送信パケットＰＫに付加するようにした。

【０１００】

この場合、送信装置２は、受信装置３から要求がない場合に識別情報ＪＰを送信パケットＪＰに付加して送信しない分だけ送信装置２自身及びインターネット５上におけるルータ等の中間ノードに対する処理負荷を低減することができる。

【０１０１】

また送信装置２は、受信装置３から要求があった期間以外は休止状態にあるようにしたことにより、当該受信装置３から要求がない場合に識別情報ＪＰを生成しない分だけ識別情報付加部１３自身の処理負荷を低減できると共に省電力化を図ることができる。

【０１０２】

一方、受信装置３は、受信手段としての受信側インターフェイス２１により、送信装置２からインターネット５を介して順次送信された送信パケットＰＫ（妨害対策パケットＢＭＰＫ）を受信し、検出手段としての攻撃検出手段２４により、当該受信した各送信パケットＰＫのうち、当該パケットの内容が変更された送信パケットである内容変更パケットＦＰＫを検出する。

【０１０３】

この状態において受信装置３は、要求手段としてのフィードバック制御部２５及びフィードバック送信部２６により、検出された内容変更パケットＦＰＫの単位攻撃回数が所定の閾値よりも上回っているときのみ識別情報ＪＰの送信パケットＰＫへの付加を送信装置２に要求するようにした。

【０１０４】

この場合、受信装置３は、送信装置２に要求しない際に送信装置２からは識別情報ＪＰの付加された妨害対策パケットＢＭＰＫが送信されない分だけ送信装置２自身及びインターネット５上におけるルータ等の中間ノードに対する処理負荷を低減することができる。

【０１０５】

ここで、受信装置３は、送信装置２と受信装置３とだけが独自に有する識別情報生成アルゴリズムに従って擬似乱数Ｇと、当該擬似乱数Ｇに対して固有なシーケンス番号Ｓとでなる識別情報ＪＰに基づいて内容変更パケットＦＰＫであるか否かを判定することにより、当該識別情報ＪＰの有無を認識する（第１段階）、或いは単に過去のシーケンス番号Ｓとの同一性や擬似乱数列Ｇとの同一性の照合するだけで内容変更パケットＦＰＫを検出することができる。

【０１０６】

この場合、受信装置３は、送信パケットＰＫの復号の際に内容変更パケットＦＰＫを検出する場合に比して処理負荷の小さい簡易な処理で当該内容変更パケットＦＰＫを検出することができ、これにより通信妨害装置４から大量の内容変更パケットＦＰＫを受信した場合であっても、処理負荷を格段に低減することができ、その結果、大量の内容変更パケットＦＰＫを受信したことによるシステムダウン等を防止することができる。

【０１０７】

また受信装置３は、複数の送信装置のうち、内容変更パケットＦＰＫに係る送信パケットＰＫを送信する送信装置２に対してのみ識別情報ＪＰの付加を要求するようにしたことにより、当該複数の送信装置全てに対して要求する場合に比してインターネット５上における処理負荷を格段に低減することができる。

【０１０８】

以上の構成によれば、当時装置である正規の送信装置２と受信装置３との間で複数の送信パケットＰＫをインターネット５を介して送受信中に、当該受信装置３に送信される内容変更パケットＦＰＫの単位攻撃回数が所定の閾値を上回っているときだけ当該各送信パケットＰＫにそれぞれ識別情報ＪＰを付加した妨害対策パケットＢＭＰＫを送受信するようにしたことにより、サービス妨害行為がなかった場合には各送信パケットＰＫにそれぞれ識別情報ＪＰを付加しない分だけ送信装置２、インターネット５上の中間ノード及び受信装置３における送受信システム１全体の処理負荷を低減することができ、かくして、システム全体としての送信効率を向上することができる。

【０１０９】

（６）他の実施の形態

上述の実施の形態においては、受信装置３が受信した内容変更パケットＦＰＫの単位攻撃回数が所定の閾値を上回ったときサービス防害対策の開始を行わせるようにした場合について述べたが、本発明はこれに限らず、当該受信装置を統括的に制御するＣＰＵの処理負荷を常時監視し、当該ＣＰＵの処理負荷が所定の閾値を上回ったときサービス防害対策の開始を行わせる等、要は、受信装置３における受信状況に応じてサービス防害対策の開始を行わせるようにすることができる。

【０１１０】

さらに上述の実施の形態においては、図６について上述した構成の要求データＤＮを適用する場合について述べたが、本発明はこれに限らず、この他種々の構成でなる要求データを本発明を適用することができる。

【０１１１】

さらに上述の実施の形態においては、要求データＤＮを送信パケットＰＫと同一のネットワークであるインターネット５を介して送信するようにした場合について述べたが、本発明はこれに限らず、要求データＤＮと送信パケットＰＫとをそれぞれ異なるネットワークを介して送受信するようにしても良く、要は、受信装置３が識別情報ＪＰの送信パケットＰＫへの付加を送信装置２に要求した際に、当該要求に送信装置２が応じるような要求手法を選定することができる。

【０１１２】

さらに上述の実施の形態においては、インターネット５上の通信プロトコルであるＩＰsec に本発明を適用する場合について述べたが、本発明はこれに限らず、例えばＳＳＨ等のインターネット上の通信プロトコル、ＬＡＮ（Local Area Network）上の通信プロトコル、衛星放送上の通信プロトコル又は文字放送上の通信プロトコル等、他のネットワーク上におけるこの他種々の通信プロトコルに本発明を適用することができる。

【０１１３】

さらに上述の実施の形態においては、送信処理部１２（図２）における送信処

理を送信プログラムによって実現すると共に、受信処理部２３（図３）における受信処理を受信プログラムによって実現するようにした場合について述べたが、本発明はこれに限らず、当該送信装置２内の各部全体の処理を当該送信プログラムによって実現するようにしても良く、また受信装置３内の各部全体の処理を当該受信プログラムによって実現するようにしても良く、当該各部をそれぞれ専用の集積回路によって実現するようにしても良い。

【０１１４】

さらに上述の実施の形態においては、プログラム格納用メモリ内に予め格納された送信プログラムに従って図７について上述した送信処理手順で送信処理を実行すると共に、当該メモリ内に予め受信プログラムに従って図８について上述した受信処理手順で受信処理を実行するようにした場合について述べたが、本発明はこれに限らず、送信プログラム及び又は受信プログラムが格納されたプログラム格納媒体から情報処理装置にインストールすることにより当該送信処理及び又は受信処理を実行するようにしても良い。

【０１１５】

この場合、かかる送信プログラム及び又は受信プログラムを情報処理装置にインストールして実行可能な状態にするためのプログラム格納媒体としては、例えばフレキシブルディスク、ＣＤ－ＲＯＭ（Compact Disk-Read Only Memory ）、ＤＶＤ（Digital Versatile Disc）等のパッケージメディアのみならず、プログラムが一時的若しくは永続的に格納される半導体メモリや磁気ディスク等で実現しても良い。またこれらプログラム格納媒体に送信プログラム及び又は受信プログラムを格納する手段として、ローカルエリアネットワークやインターネット、ディジタル衛星放送等の有線又は無線通信媒体を利用しても良く、ルータやモデム等の各種通信インターフェースを介して格納するようにしても良い。

【０１１６】

【発明の効果】

上述のように本発明によれば、所定の通信プロトコルに準拠して生成された送信パケットを順次ネットワークを介して送信し、当該送信パケットの送信対象である受信側から要求があった期間のみ、当該受信側だけに識別させるための識別

情報を各送信パケットに付加するようにしたことにより、受信側から要求があった期間以外については識別情報を各送信パケットに付加しない分だけ送信手段、識別情報付加手段及びネットワーク上に介在する中間ノードに対する処理負荷を低減することができ、かくして、システム全体としての送信効率を向上することができる。

【０１１７】

また、上述のように本発明によれば、送信側からネットワークを介して順次送信され、所定の通信プロトコルに準拠した送信パケットを受信し、当該受信された各送信パケットのうち、当該パケットの内容が変更された送信パケットである内容変更パケットを検出し、当該検出した内容変更パケットの受信状況に応じて、検出手段だけに識別させるための識別情報の送信パケットへの付加を送信側に要求するようにしたことにより、送信側に要求しない際に送信側からは識別情報の付加された送信パケットが送信されない分だけ送信装置及びネットワーク上に介在する中間ノードに対する処理負荷を低減することができ、かくして、システム全体としての送信効率を向上することができる。

【図面の簡単な説明】

【図１】

本発明を適用した送受信システムの全体構成を示す略線図である。

【図２】

送信装置の構成を示すブロック図である。

【図３】

妨害対策パケットの構成を示す略線図である。

【図４】

識別情報の構成を示す略線図である。

【図５】

受信装置の構成を示すブロック図である。

【図６】

要求データの構成を示す略線図である。

【図７】

送信処理手順を示すフローチャートである。

【図８】

受信処理手順を示すフローチャートである。

【符号の説明】

１……送受信システム、２……送信装置、３……受信装置、４……通信妨害装置、１２……送信処理部、１３……識別情報付加部、１４……フィードバック受信部、２４……攻撃検出部、２５……フィードバック制御部、２６……フィードバック送信部。

【書類名】図面

【図１】

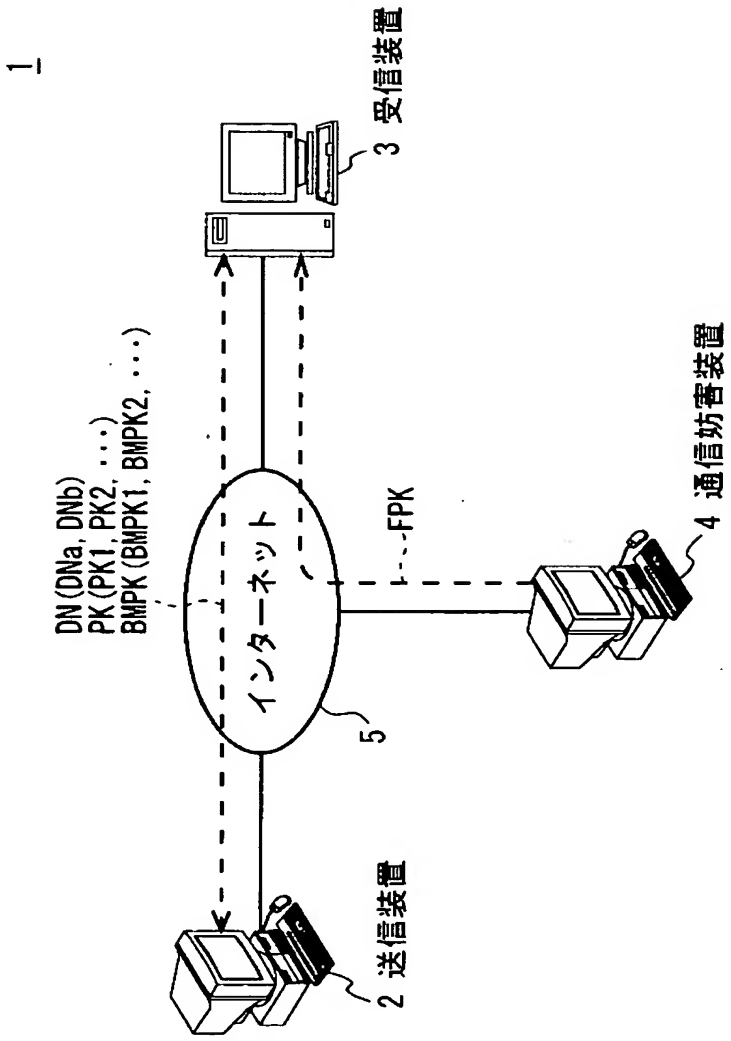

図１　送受信システムの全体構成

【図２】

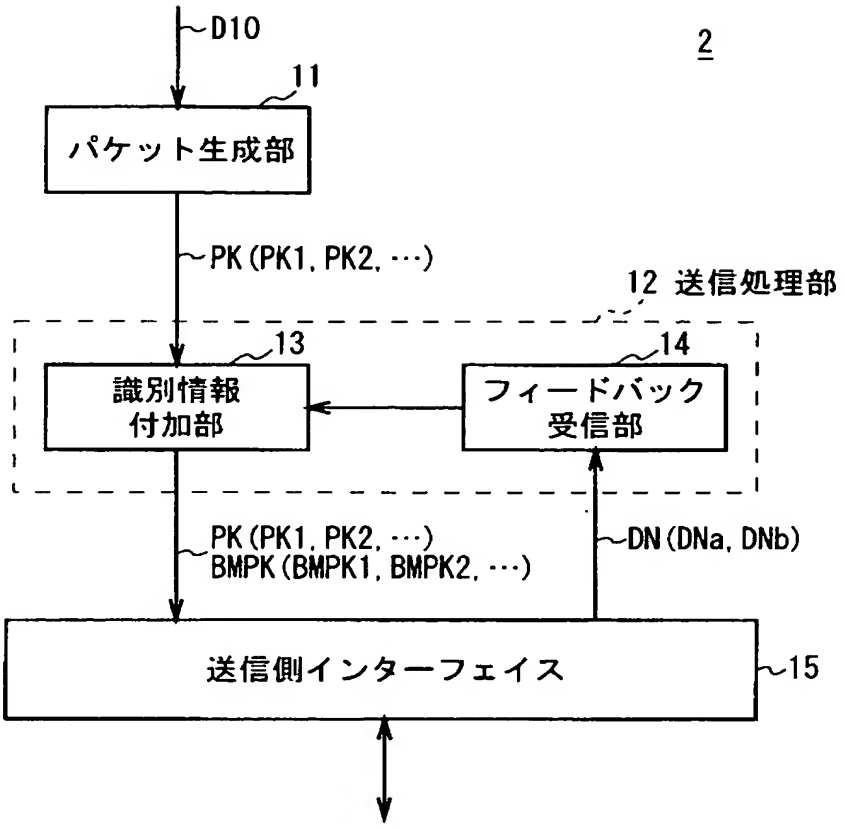

図２　送信装置の構成

【図３】

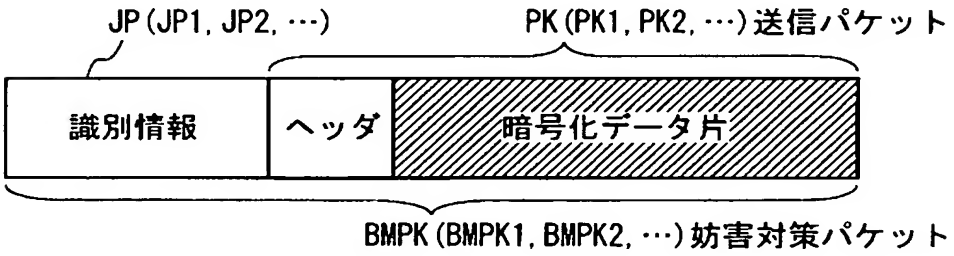

図３　妨害対策パケットの構成

【図４】

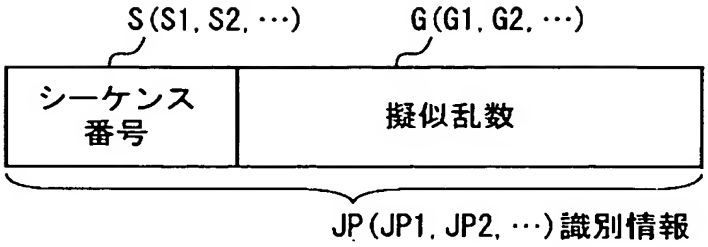

図４　識別情報の構成

【図５】

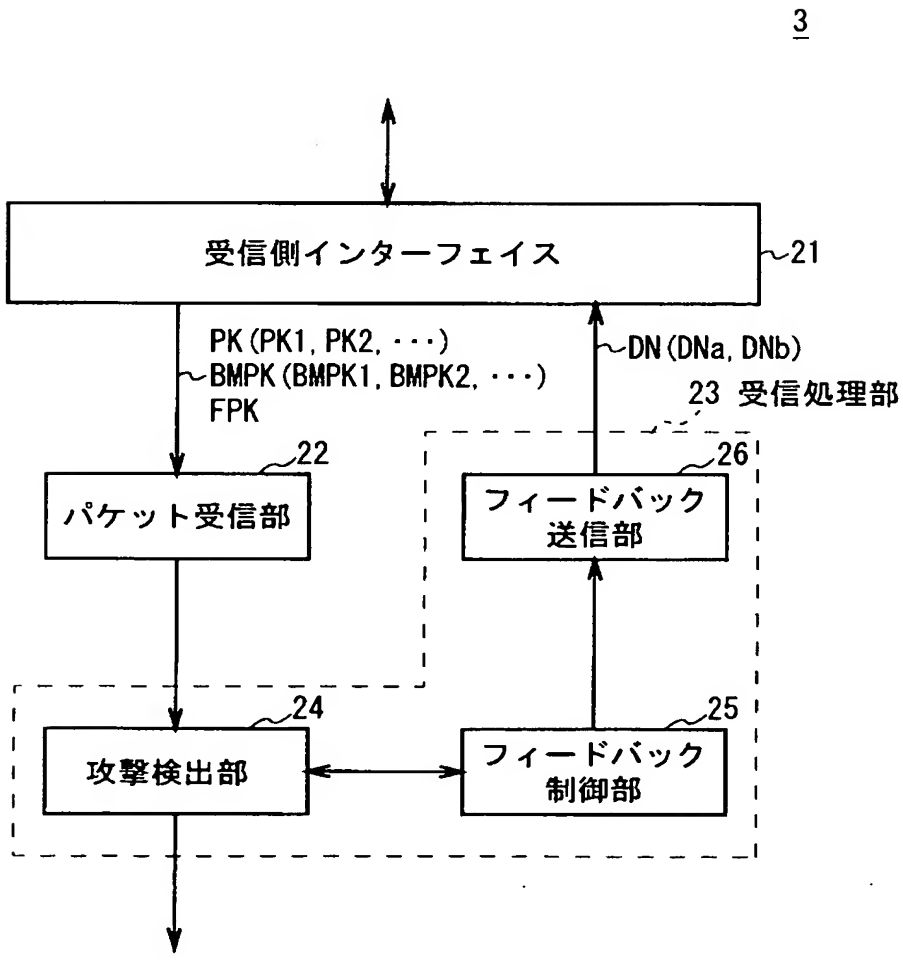

図５　受信装置の構成

【図６】

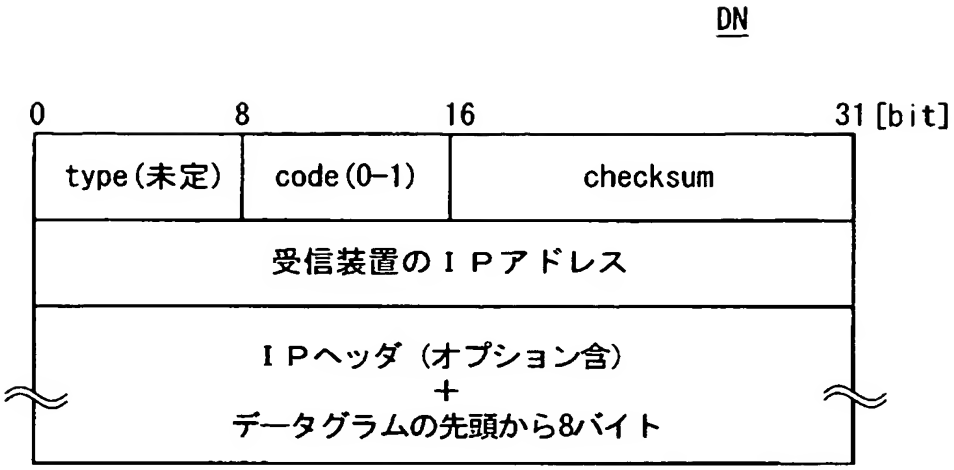

図６　要求データの構成

【図７】

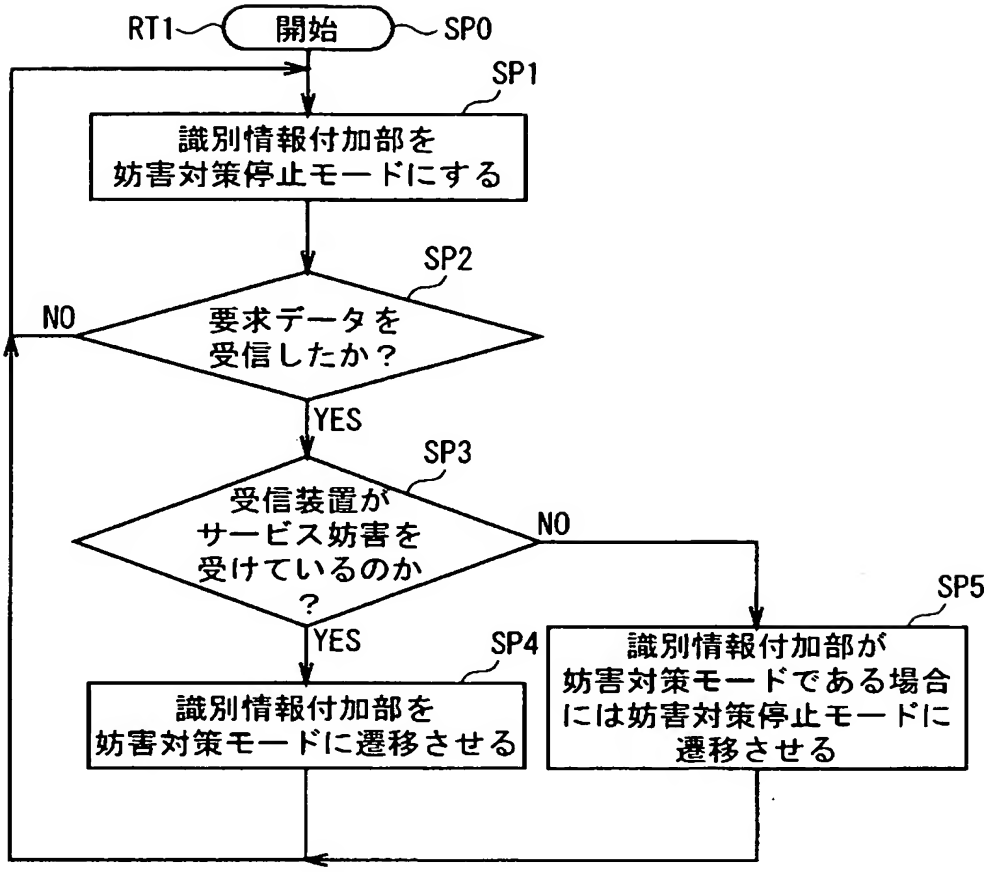
RT1
開始
SP0
SP1
識別情報付加部を
妨害対策停止モードにする
SP2
NO
要求データを
受信したか？
YES
SP3
受信装置が
サービス妨害を
受けているのか
？
NO
SP5
YES
SP4
識別情報付加部を
妨害対策モードに遷移させる
識別情報付加部が
妨害対策モードである場合
には妨害対策停止モードに
遷移させる

図７　送信処理手順

【図８】

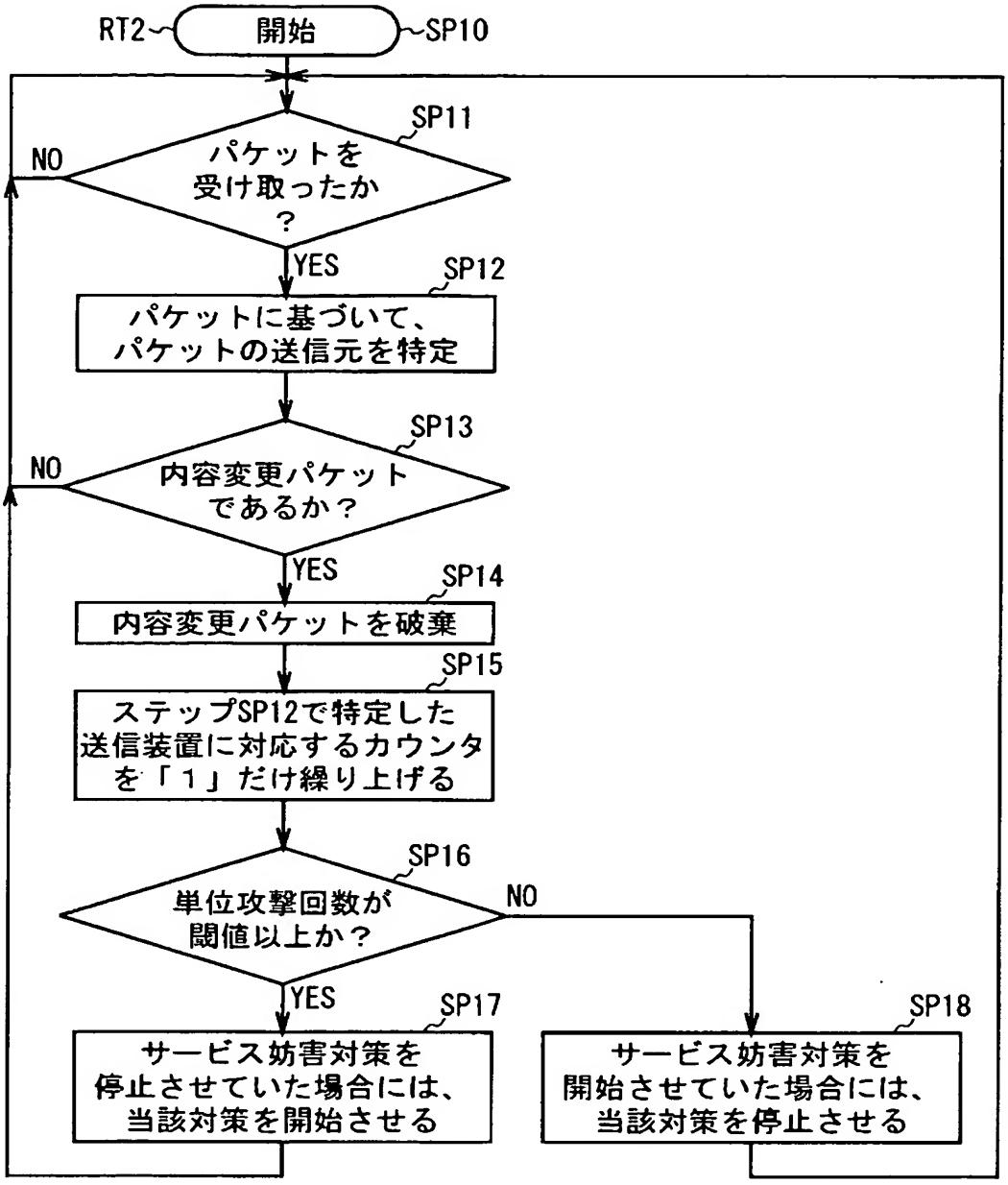
RT2
開始
SP10
SP11
パケットを
受け取ったか
？
NO
YES
SP12
パケットに基づいて、
パケットの送信元を特定
SP13
内容変更パケット
であるか？
NO
YES
SP14
内容変更パケットを破棄
SP15
ステップSP12で特定した
送信装置に対応するカウンタ
を「１」だけ繰り上げる
SP16
単位攻撃回数が
閾値以上か？
NO
YES
SP17
サービス妨害対策を
停止させていた場合には、
当該対策を開始させる
SP18
サービス妨害対策を
開始させていた場合には、
当該対策を停止させる

図８　受信処理手順

【書類名】　　要約書

【要約】

【課題】

本発明は、システム全体としての送信効率を向上できるようにする。

【解決手段】

本発明は、正規の送信装置２と受信装置３との間で複数の送信パケットＰＫをインターネット５を介して送受信中に、当該受信装置３に送信される内容変更パケットＦＰＫの単位攻撃回数が所定の閾値を上回っているときだけ当該各送信パケットＰＫにそれぞれ識別情報ＪＰを付加した妨害対策パケットＢＭＰＫを送受信することにより、サービス妨害行為がなかった場合には各送信パケットＰＫにそれぞれ識別情報ＪＰを付加しない分だけ送信装置２、インターネット５上の中間ノード及び受信装置３における処理負荷を低減することができ、かくして、送受信システム１全体としての送信効率を向上することができる。

【選択図】　　図１

特願２００３－０１６６４１

出　願　人　履　歴　情　報

識別番号　　［０００００２１８５］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社